CWIN | Critical infrastructure Warning Information Network

CWINReport

Summer 2004 Vol. II, No. 2

A National Security and Emergency Preparedness (NS/EP) Support Program of the National Communications System

In This Issue

NSIE Meets CWIN

CWIN Security Dimension Discussed with NSTAC Information Exchange Group

In May, An Nguyen, senior electronics engineer for the National Communications System (NCS), briefed the Critical infrastructure Warning Information Network (CWIN) to one of the scientific groups sponsored by the President's National Security Telecommunications Advisory Committee (NSTAC), the Network Security Information Exchanges (NSIE). The focus of the presentation was CWIN security, but the discussion included a range of topics concerning the nature of the network.

The NSIE representatives include subject matter experts, from Government Departments and Agencies as well as private industry, who are engaged in prevention and/or investigation of telecommunications software penetrations or have security responsibilities. In addition to Government representatives, membership from private industry includes telecommunications carriers and major users.

continued on page 3

CWIN Receives Authority to Operate

The NCS recently awarded to CWIN the authority to operate for three years up to April 15, 2007. The decision was based on the conclusion of an extensive security test and evaluation process performed on CWIN by representatives from the Defense Information Systems Agency (DISA). The approval process included interviews with system administrators and program personnel, review of appropriate documentation, operating system scans, audits and

continued on page 3

First CWIN Users' Forum Held

On February 24, 2004, the first CWIN Users' Forum was held at the National Communications System (NCS) headquarters in Washington, DC. Altogether, 11 CWIN members gathered, including representatives from the NCS, the National Coordination Center for Telecommunications-Information Sharing and Analysis Center, Department of Energy, Computer Emergency Response Team – Coordination Center, Infrastructure Coordination Division (ICD), National Cyber Security Division and Verizon.

continued on page 4

Using the Conference Bridge

As announced in the previous newsletter, CWIN now has its own dedicated conference bridges. A conference bridge allows multiple users to dial into a central location using either the Voice over Internet Protocol (VoIP) phone or an analog phone from the public network. The conference bridge provides a secure conference calling capability.

If you receive a notification that a conference call will be held, do you know what to do? Here are procedures to get started.

1. An NCS member will initiate the conference call.
2. An NCS member will contact the necessary participants via e-mail or phone and provide the time and date of the conference.
3. The NCS' phone call or e-mail announcing the conference call will contain a PASSCODE number. A PASSCODE defines the specific conference to which the user belongs.
4. To identify yourself to the conference bridge, you may be required to enter a personal identification number (PIN), which you will receive from the NCS administrator via e-mail. The PIN allows you to access the system.
5. If you lose your PASS-CODE or PIN (or you believe either has been compromised), you will not be allowed to use the conference bridge. (Contact the CWIN Program Manager immediately to generate a new PASSCODE or PIN.)
6. At the predetermined time of conference, pick up the VoIP phone and dial the appropriate access numbers. Enter the conference PASS-CODE and PIN if applicable.
7. You have now entered a conference.

Typically, it will take an authorized user less than 30 seconds to connect to a conference. If you have any questions or concerns, contact the CWIN Program Manager.

CWIN Evades Bot

On April 6, 2004, an undisclosed source notified the National Coordinating Center for Telecommunications Information Sharing and Analysis Center (NCC-Telecom ISAC) of a malicious bot network attack affecting 12,000 computers. A bot (a slang term for an autonomous program used by hackers) is a Trojan virus infecting Internet hosts; the attacker remotely controls the host via private Internet relay chat protocol. In this case, a miscreant tapped into a network, subverting it and used it inappropriately under the guise of the original network owner.

The NCC Watch notified the Telecom ISAC of the attack through a teleconference and informed the members that an e-mail would be sent with details and suggested courses of action. One of the members of the Telecom ISAC reported technical difficulty receiving the e-mail through the server at its network operations center.

Nate Wann, the senior information assurance engineer who was the active watch officer at the time, recommended sending the alert over the CWIN to the organization suffering the e-mail disruption. CWIN quickly delivered the information to the receiving organization. Wann commented there is definitely a "need to build CWIN into daily procedures, creating a redundant path and ensuring critical information gets to its destination during emergencies."

This is a prime example of the type of event for which CWIN is designed; a network ready when it's needed, when other networks are suffering disruptions.

NSIE *continued from page 1*

The NSIE members were particularly interested to learn of the measures that have been taken to protect the network from the disruptions of the public Internet and the public switched network (PSN). Mr. Nguyen stated that CWIN is separate and isolated from the PSN and the Internet by design. The CWIN security posture is defense in-depth with multiple levels of protection throughout the infrastructure as well as the network backbone upon which its traffic rides. For example, data traffic is separated using multi protocol label switching/virtual private network (MPLS/VPN), which uses the best of frame relay-style (an industry-recognized overlay networking technology) security and VPN concepts to ensure data security.

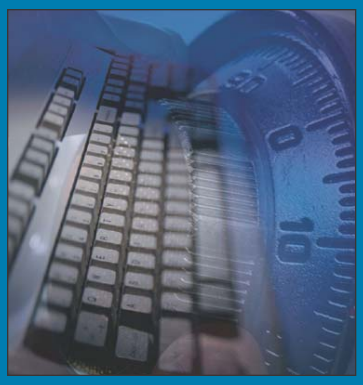
In addition, the network includes redundancy and diversification. If one of the users loses connectivity, the rest of the network continues to operate without disruption. Furthermore, diverse circuits connect the data centers, ensuring trouble-free operations even if one of the circuits is lost. CWIN is based on a highly fault-tolerant, resilient national carrier infrastructure.

Following the lively discussion, the NSIE representatives thanked Nguyen and the CWIN team for their participation.

Operating Authority *continued from page 1*

system checks. The security testing verified that the security posture of CWIN meets the required Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and national information assurance guidance and requirements.

All Federal information technology systems are required to receive certification and authorization to operate; this is CWIN's first such certification and marks a milestone in its implementation.



Security Lockdown:

Unattended Workstations

Did you leave the front door unlocked? Most of us wouldn't dream of leaving the house and not making sure the front door was locked. But how many times during the workday do you log into a computer and get up to get some coffee or a glass of water and leave your workstation logged in?

One of the main ways that a hacker, or even a fellow co-worker, can gain illegitimate access to files is by waiting until someone leaves a logged in workstation unattended.

In sensitive Government installations, the situation can have even greater repercussions. Fortunately, most computer systems in security-conscious environments in the U.S. have policies that prohibit leaving a logged in workstation. Some installations even have systems in place that log you out when sensors determine that you have gone more than a foot from your PC. Yep, that's right...just like in the Hollywood movies.

CWIN is a sophisticated computer network with self-defense mechanisms that can handle just about any kind of threat, but for now, leaving a logged in workstation unprotected is the responsibility of the people that operate the terminals.

Some simple rules to follow:

1) If you can't see the screen, you're too far away.
2) Logged in and unattended equals vulnerable.
3) If you're going to be away for more than one minute, lock the workstation.

Welcome Kevin C. Piekarski, CWIN Program Manager

Kevin C. Piekarski is the new CWIN Program Manager, bringing depth to the program with experience that spans both the private sector and Federal service. He joined NCS in 2002 as an Information Technology Specialist in information security. His background spans 15 years including 10 years as a Data Systems Technician in the Navy and positions in IT and telecom with BBN, Verizon Federal Network Systems, iDirect Inc. and the Department of State (DOS).

Noting that the CWIN is a key component within the Department of Homeland Security, he commented, "My job is to make sure that the CWIN continues to evolve by applying the best technologies and expanding its membership to ensure that all of the critical infrastructure sectors are included."

Among Piekarski's career highlights, he spearheaded a mission to provide Department of Defense (DOD) and DOS commands remote access to the DOD Non-classified Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET). This activity provided support to the Navy during the attack on the USS Cole in 2000.

Piekarski sees the network's value to the NCS and its customers. "The CWIN is a vehicle for Government and industry decision-makers to share critical infrastructure information."

Forum *continued from page 1*

The half-day forum provided a platform for feedback on the mission and the CWIN Standard Operating Procedures for CWIN as well as ideas for an upcoming CWIN Significant Events Conference exercise to be held later this year. In addition, the forum attendees talked about the value that the network can provide, given its mission's expanded scope. Jim Kliner, a senior policy analyst who is a contractor providing support to the ICD noted, "CWIN provides a valuable opportunity for collaboration among Government, industry and Information Sharing and Analysis Centers."

The next CWIN Users' Forum is tentatively scheduled for September 28, 2004. The daylong forum will be open to the entire CWIN community and will include briefings on technical, operational and policy issues as well as provide an opportunity for discussion and feedback. The CWIN Program Manager will provide users detailed information in the upcoming months.

Important Dates

Monthly Test - 3rd Monday of each month

CWIN Program Manager

Tel: 1-866-NCS-CALL (1-866-627-2255)
1-703-676-CALL (703-676-2255) DC Metro Area
E-mail: cwin@ncs.gov
Web: www.ncs.gov

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
National Communications System
701 South Courthouse Road
Arlington, VA 22204-2198

24/7 Help Desk:
1-877- 441-9330

Technical Support: Service Management Center (SMC)

VoIP Phone Ext: 4357 (HELP)
Tel: 1-877-441-9330 (Toll Free)
E-mail: smc@arrowhead.com
CWIN E-mail: ncc.help